Cyber Deterrence, Cyber Response and Defence of the Digital Nation / Economy

Emeritus Professor William J (Bill) Caelli, AO
Director – International Information Security Consultants Pty Ltd
Member – Independent Scholars Association of Australia

Presentation to the AusCERT-2012 Conference
Gold Coast, Queensland.
Australia.
16 May 2012.

ACKNOWLEDGEMENT:

This further research follows on from the first stage work done and published under the *"Protecting critical infrastructure from denial of service attacks"* Project TA020002 - funded under the Australia-India Strategic Research Fund (AISRF), Department of Innovation, Industry, Science and Research **

QUT researchers on sub-project in TA020002 / 2008-2011 were:

- Emeritus Professor William J (Bill) Caelli, AO – QUT/ISI
- Ms J Georgiades – QUT / Faculty of Law
- Professor William Duncan – QUT / Faculty of Law
- Professor Sharon Christensen – QUT / Faculty of Law

Indian researchers on sub-project in TA020002 / 2008-2011 were:

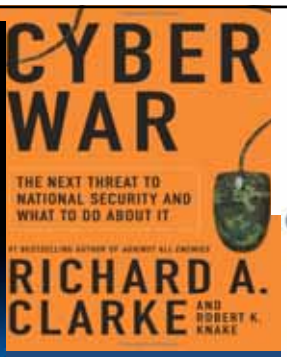
- Professor S V Raghavan – Indian Institute of Technology, Chennai.
- Mr S M Bhaskar - TCS

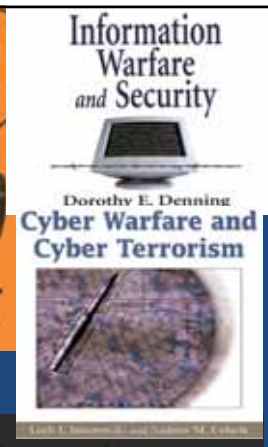
** Note: new Departmental designation as of December 2011

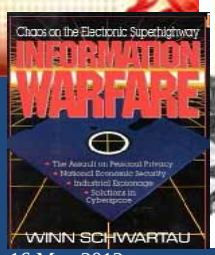
Si vis pacem, para bellum

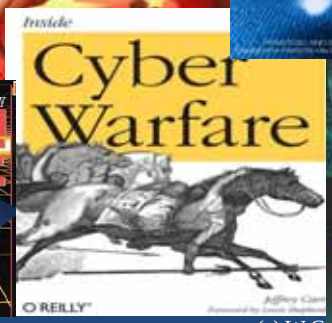
If you wish for peace,
prepare for war

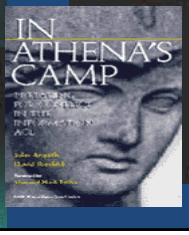
16 May 2012 (c) W Caelli - IISEC Pty Ltd 3











16 May 2012 (c) W Caelli - IISEC Pty Ltd 4

The mission of the United States Air Force is to fly, fight and win...

in air, space and cyberspace.

http://www.af.mil/main/welcome.asp April 2012

SFGate home of the San Francisco Chronicle

ANZUS

Secretary of Defense USA

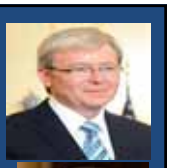
Leon Panetta

*"Cyber is the battlefield of the future," Panetta told reporters traveling on his plane. "We are all going to have to work very hard not only to defend against cyber attacks but to be **aggressive** with regards to **cyber attacks** as well. The best way to accomplish that is not only on our own, but working with our partners."*

Read more: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/09/14/bloomberg1376-LRJE970YHQ0X01-0MUBUS4IR8TG1N6J027E4V9GAK.DTL#ixzz1Y5Hlr4LL

Cyber War Added to Threats Under U.S., Australia Defense Treaty, Wednesday, September 14, 2011

The Hon Kevin Rudd MP
Former Minister for Foreign Affairs




Cooperation on Cyber – a new dimension of the US Alliance

Joint media release : The Hon Kevin Rudd MP, Minister for Foreign Affairs & The Hon Stephen Smith MP, Minister for Defence, 15 September 2011

*The US and Australian Governments agreed today that a **cyber attack** on either of them would trigger the mechanisms of the **ANZUS** Treaty.*

26th Australia-United States Ministerial Consultations (AUSMIN) September 15, 2011

16 May 2012 (c) W Caelli - IISEC Pty Ltd 7

General Keith Alexander
Director, National Security Agency
Chief, Central Security Service
Commander, United States Cyber Command (USCYBERCOM).

- *…congressional hearing … rampant cyber-theft involved "the greatest transfer of wealth in history"* AFR 5 Apr 2012

16 May 2012 (c) W Caelli - IISEC Pty Ltd 8

CHINA

July 2010

PLA's General Staff Department (GSD) announces

"Information Security Base"

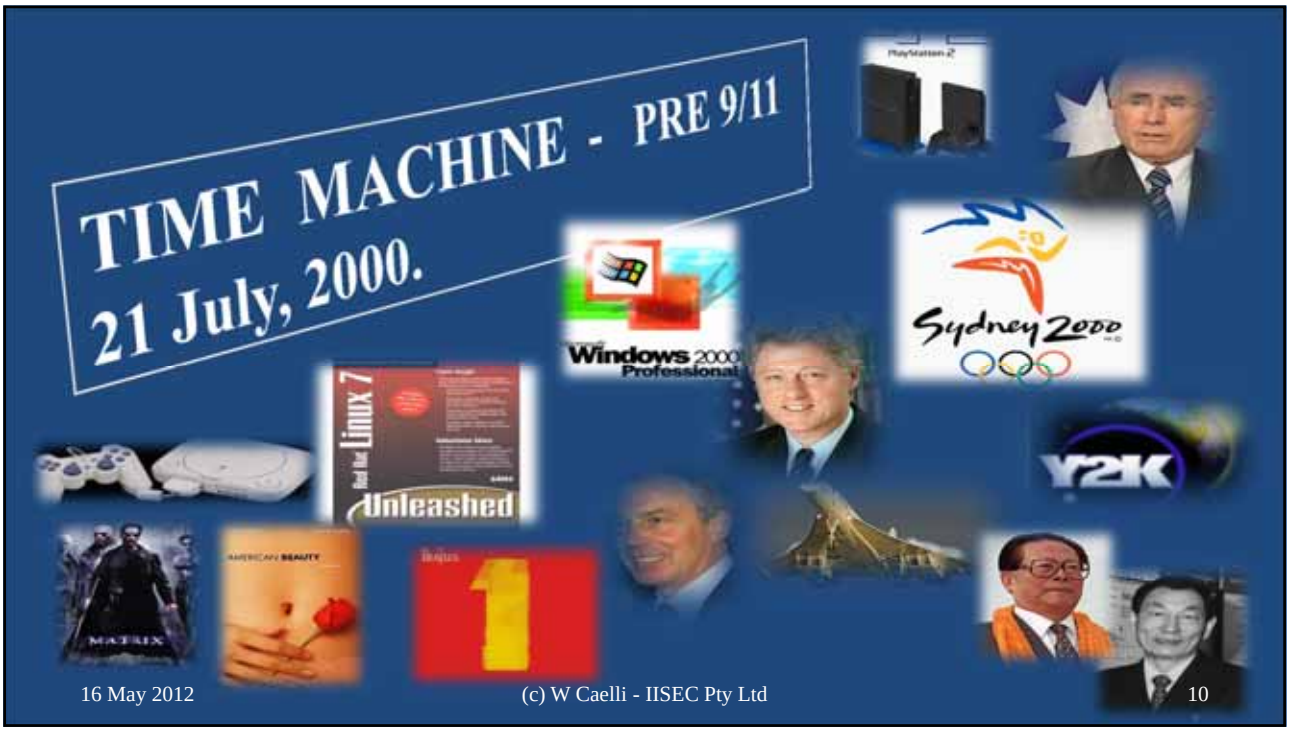
Ordered by President Hu Jintao

"….our army is strengthening its capacity and is developing potential military officers to tackle information –based warfare.."

Source:

William T Hagestad II, *"21st Century Chinese Cyberwarfare"* , UK 2012

16 May 2012 (c) W Caelli - IISEC Pty Ltd 9



16 May 2012 (c) W Caelli - IISEC Pty Ltd 10

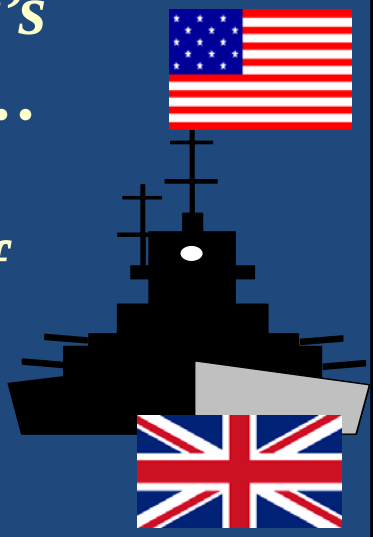
21 July 2000

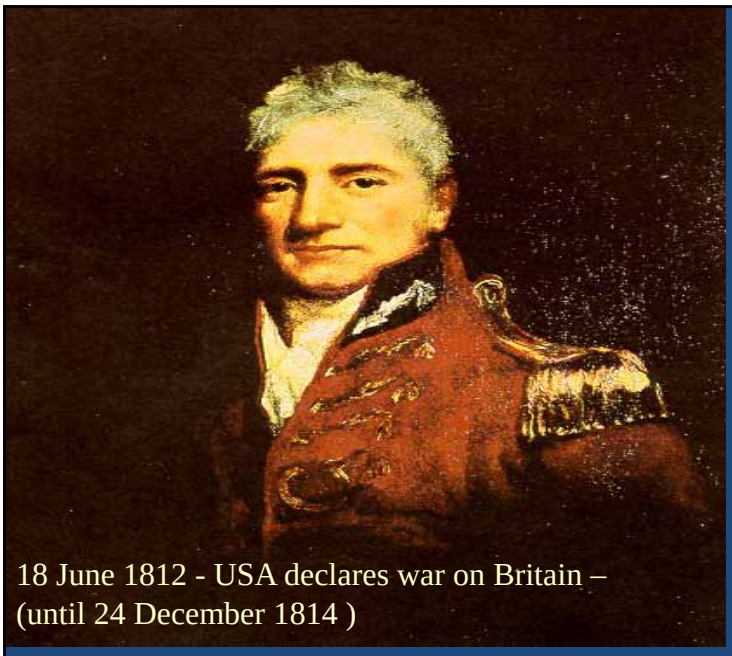
"In the Information World, What are the Responsibilities of Government, Law Enforcement and the Citizen ?"

W. J. Caelli

2nd Commonwealth Investigators' Conference
" Partnerships and Technology in the Fight Against Crime"
Bardon Professional Centre, Brisbane. Qld. 21 July 2000

" … in order that His Majesty's Subjects may do their utmost … to.. capture .. the Ships and Vessels belonging to citizens of the United States, and to destroy their commerce…"





18 June 1812 - USA declares war on Britain – (until 24 December 1814)

Circular despatch from Earl Bathurst to Governor Macquarie, New South Wales, 13 October 1812.

Acknowledged by Governor Macquarie, 28th June 1813.

16 May 2012 (c) W Caelli - IISEC Pty Ltd 13

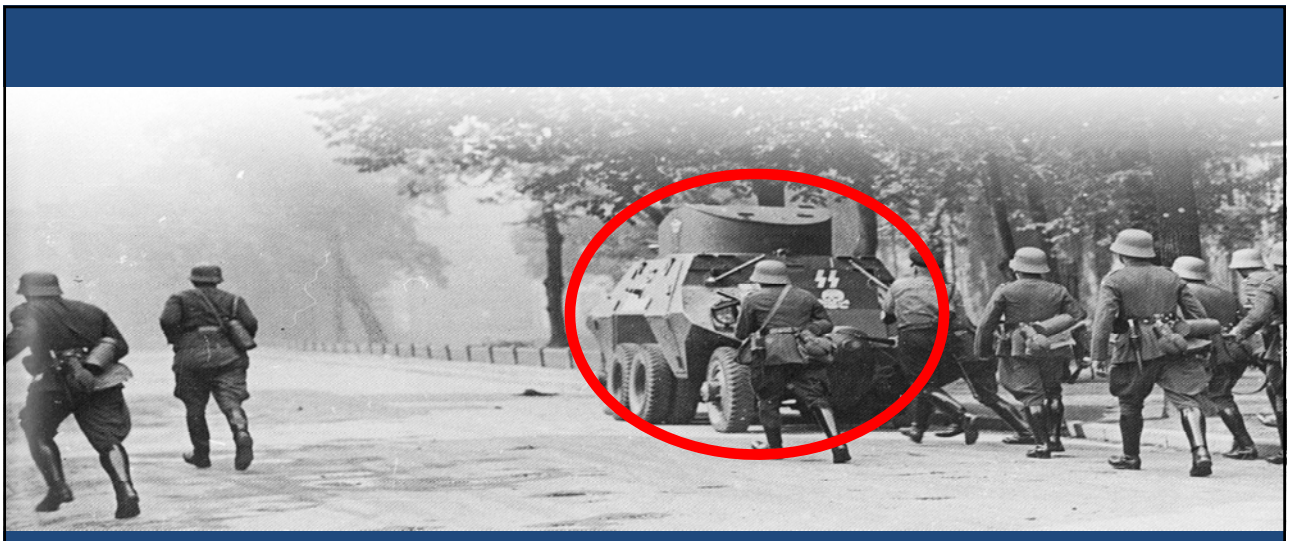
Gdansk - Danzig

Gdansk (Danzig)

16 May 2012 (c) W Caelli - IISEC Pty Ltd 14

Polish Army on exercise – late 1939

16 May 2012 (c) W Caelli - IISEC Pty Ltd 15



German SS troops enter Danzig, Poland – late 1939.

16 May 2012 (c) W Caelli - IISEC Pty Ltd 16

LONG TRADITION - ELECTRONIC WARFARE

By the end of 1944, 462 Squadron had joined 100 (Bomber Support) Group, and following the fitment of specialised radio equipment, began operations to disrupt the highly organised German air defence system. The Halifax's were modified to carry ***special radar jamming equipment designed to interfere with both the night fighter and ground based radar.***

RAAF
462 Squadron

http://www.airforce.gov.au/raafmuseum/research/units/462sqn.htm

PRESIDENT'S COMMISSION *on* CRITICAL INFRASTRUCTURE PROTECTION

Robert T Marsh, Chairman

- Formed **July 1996**
- Final Report 20 October, 1997
- Whitehouse Statement
  22 October 1997

Richard A Clarke - USA

National Coordinator for Security, Infrastructure Protection and Counter-terrorism

".. the conclusion by the Administration is that the nation IS at risk because over the last decade we have made the nation, the economy and national defense dependent upon computer networks. We have designed, ad hoc, a national information infrastructure without any thought of including security." (Clarke, May 1999)

Michael J Jacobs
Deputy Director, ISSO - NSA (USA)

"In the cyber era, our traditional lines of defense no longer provide a wall between citizens and those who would do harm."

3rd National Colloquium on INFOSEC Education
New York, USA. 25-27 May 1999

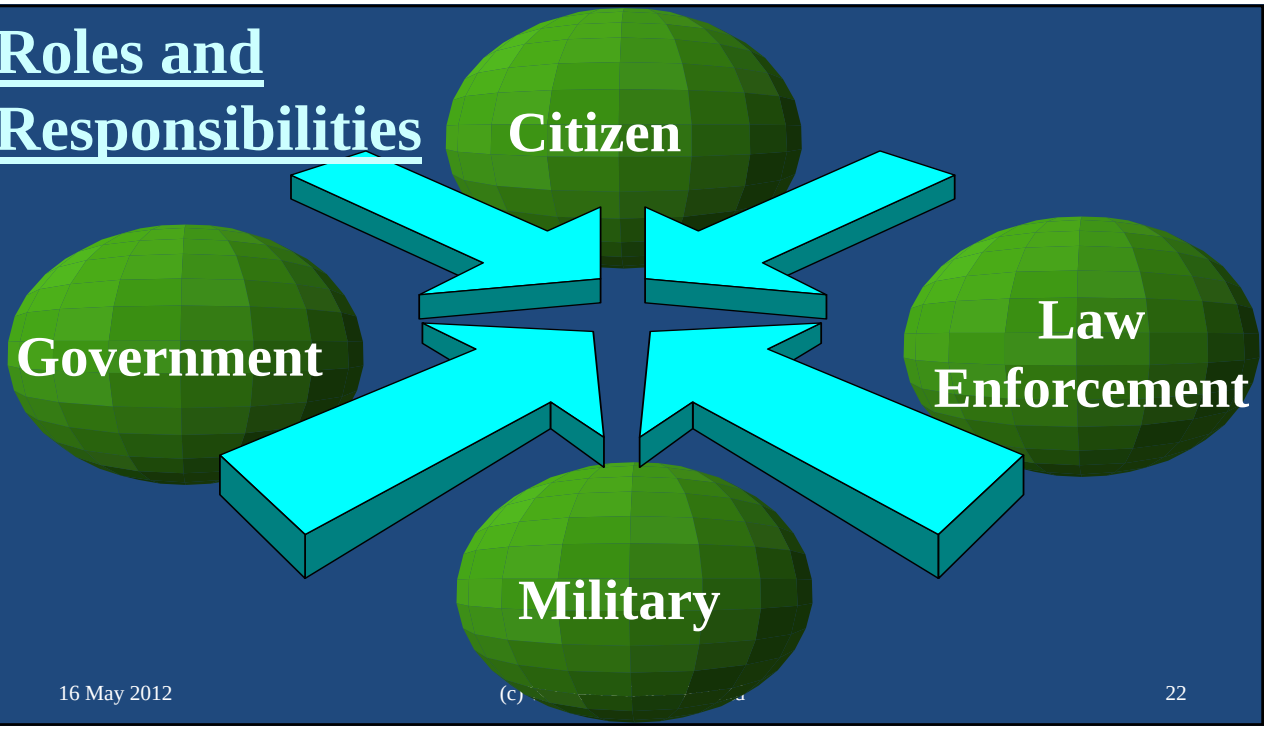
…….. a number of foreign nations have developed information-warfare doctrine, programs, and capabilities for use against the U.S. and other nations……..

2005

Louis J Freeh,
5th Director,
USA FBI
1993 - 2001

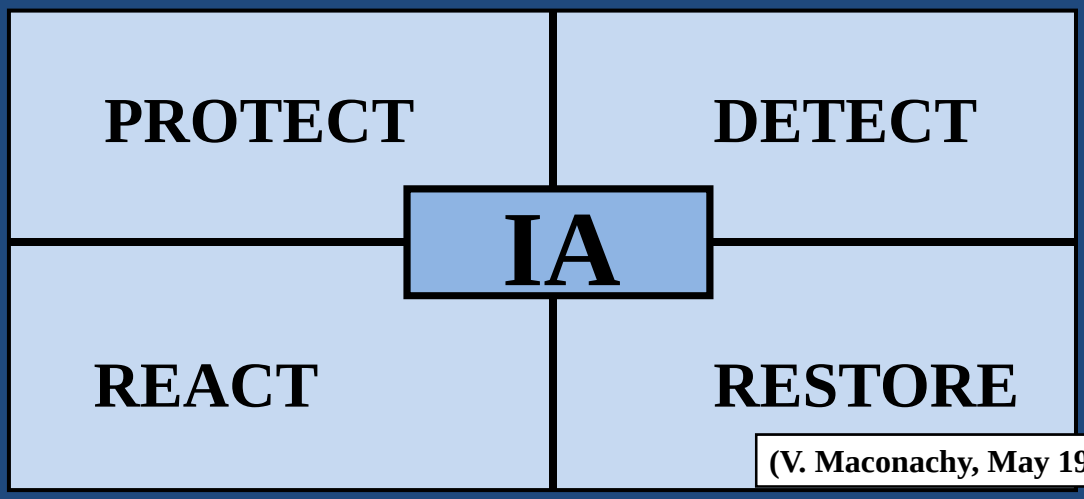
16 May 2012 (c) W Caelli - IISEC Pty Ltd 21

Roles and Responsibilities



16 May 2012 (c) [illegible] 22

FROM INFOSEC TO INFORMATION ASSURANCE (IA)

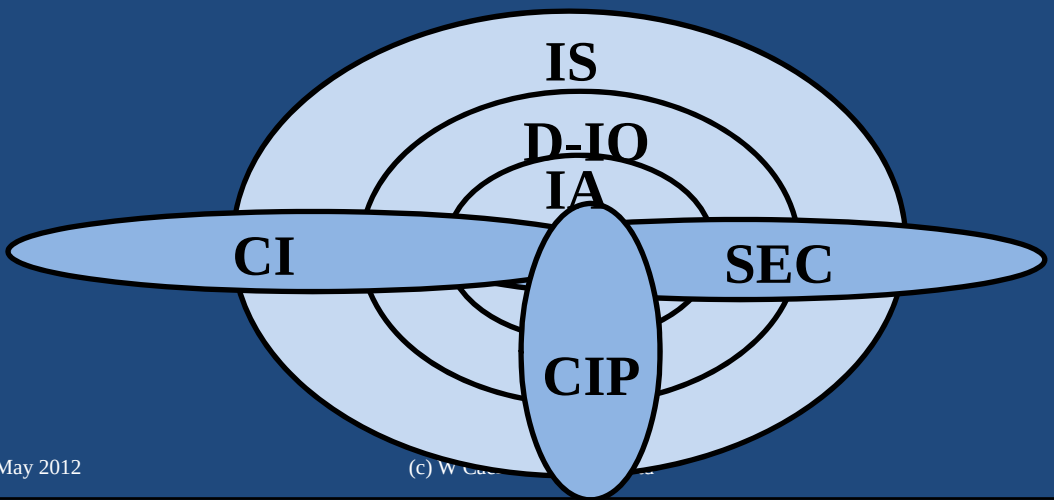


(V. Maconachy, May 1999)

16 May 2012 (c) W Caelli - IISEC Pty Ltd 23

USA - DEFENCE VIEW - 1999

DEFENSIVE INFORMATION OPERATIONS D-IO

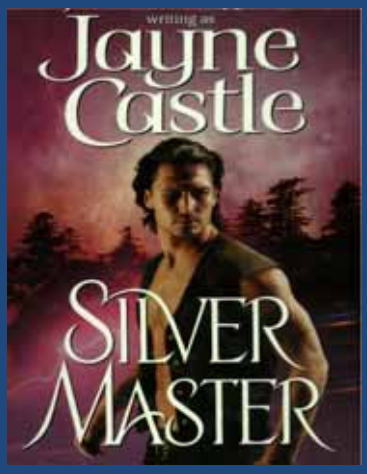


16 May 2012 (c) W [illegible] 24

EAST INDIA COMPANY

*….the capture of India was not accomplished by the British Army, but by the **private armies** of the **East India Company**, which grew in size to become larger than that of any European sovereign state……..*

Even in romantic fiction…….



*The guilds are, however, peculiar blends of **business corporations** and emerging **militia**……*

DETERRENCE…… DEFENCE ALONE

16 May 2012 (c) W Caelli - IISEC Pty Ltd 27

DETERRENCE…… OFFENCE / RETALIATION

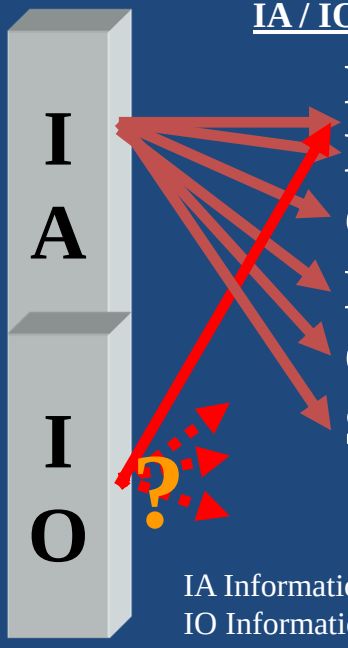
16 May 2012 (c) W Caelli - IISEC Pty Ltd 28

DETERRENCE

MUTUALLY ASSURED DESTRUCTION TO DISRUPTION ??

16 May 2012 (c) W Caelli - IISEC Pty Ltd 29

IA / IO AWARENESS, TRAINING, EDUCATION

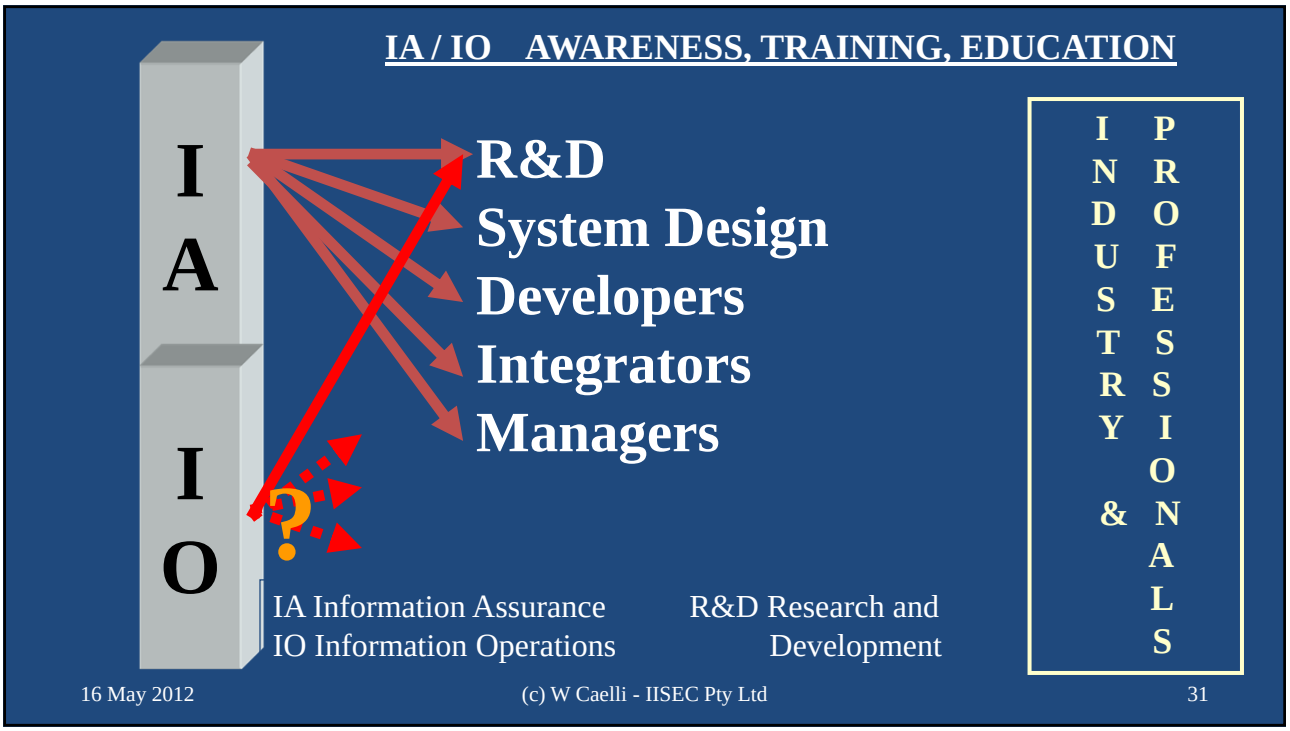


- Defence / Intelligence
- Law Enforcement
- Government
- NCI Operators
- Corporates
- SME - Citizens

U S E R S

IA Information Assurance
IO Information Operations
CNI Critical National Infrastructure
SME Small/medium enterprises

16 May 2012 (c) W Caelli - IISEC Pty Ltd 30

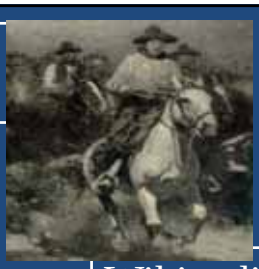


ISPs = YOUR NEW NEIGHBOURHOOD INTERNET MILITIA ?

- enforce industry determined "code" (iCode / IIA)
  - not part of any legal structure ?
  - not subject to traditional legal processes (magistrate)
- apply determined penalty (new "*sheriff / bailiff*")
  - override any pre-existing contract ?
  - enter premises to assist in compliance "obligations"
- no responsibility on system supplier
- no responsibility on service provider
  (now new "*sheriff*")

16 May 2012 (c) W Caelli - IISEC Pty Ltd 32

Posse comitatus



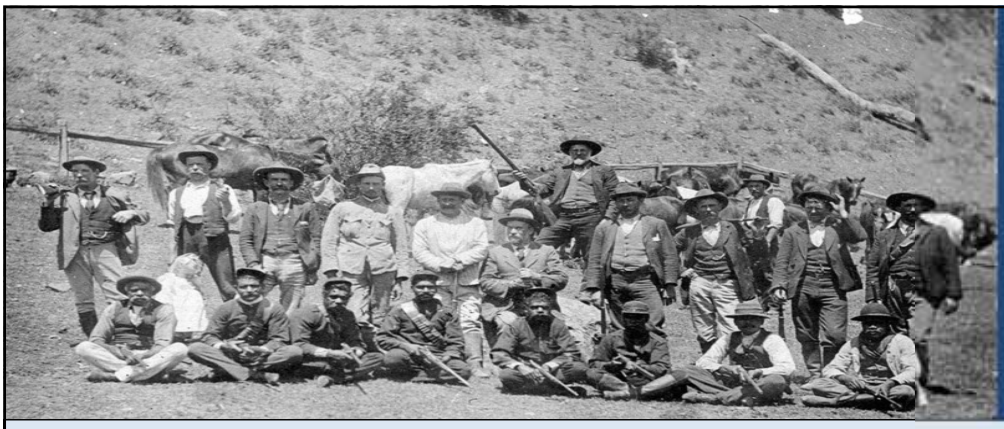
Wikipedia

- *Posse comitatus* or *sheriff's posse*
  - common-law or statute law authority of a
  - county sheriff / law officer to conscript
  - any able-bodied males to assist in
    - keeping the peace or to pursue and arrest a felon…..

- Exists in US States that have not repealed this function
- Note :
  - USA ***"Posse Comitatus Act - 1878"*** (Boston massacre – 1770)
  - no use of army / air force (1956)
  - Navy / Marines (no - but only by self regulation)
  - Coast Guard / National Guard OK
    - no Australian equivalent (differing history)

US ACT

16 May 2012 (c) W Caelli - IISEC Pty Ltd 33



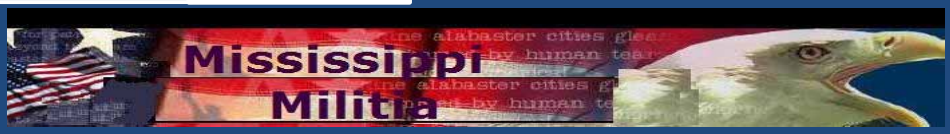
1900 Posse NSW

The hunt for the Governor gang of bushrangers.

A **posse** of mounted police, aboriginal trackers and **district volunteers.** Jimmy & Joe Governor were sighted at Stewarts Brook on 12 September 1900.

16 May 2012 (c) W Caelli - IISEC Pty Ltd 34

MILITIA USA



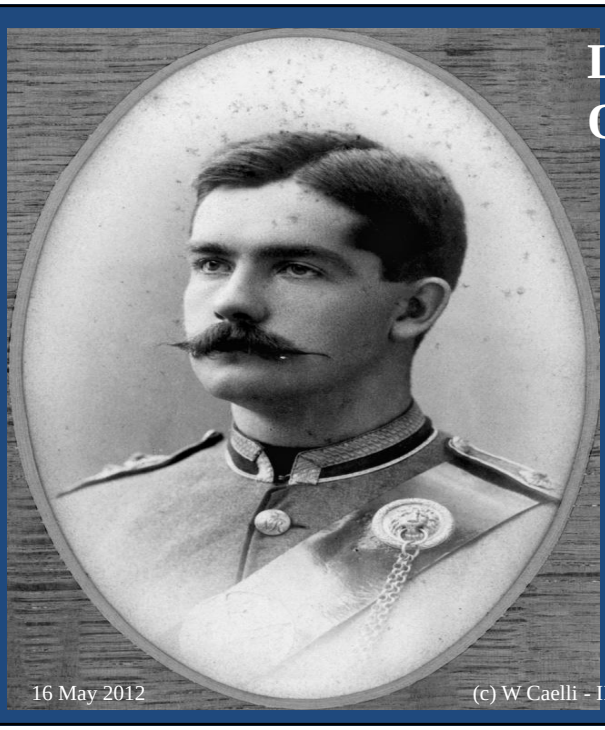
The early colonists of America considered the militia an important social structure, necessary to provide defense and public safety. (Wikipedia)

MILITIA AUSTRALIA

Citizen's Military Forces (CMF) – 1901/1980 (Reserves) **(Wikipedia)**

Queensland Navy Gunship *"Paluma"* ?

Colonial Militia – pre 1901
1855 – 1890 : Colonial government
1870 – British military control ceases
Governor – raise military / naval forces



Lieut. Richard Dowse
Queensland Volunteer Rifles
Date:1889

9th Battalion,
The Royal Queensland Regiment
(9 RQR) (1911)

DIMENSIONS & DISTINCTIONS

Vulnerability
Threat
Attack
Penetration
Compromise
Damage
Audit
Forensics

Categories:

A) individual, normal, commercial business systems

B) national critical infrastructure (NCI)

C) defence / intelligence / law enforcement / government systems

USA – FERC – LEGISLATIVE RESPONSE

FERC
FEDERAL ENERGY REGULATORY COMMISSION

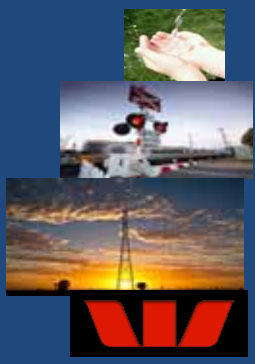
- responsibility – assurance / security
- defence / counter-measures
- response

VICTIMS

- little policy / legal recourse
- best practice guides / non-binding
- Reidenberg:
  - Civilian self-help / Strike-back
  - Supplement law-enforcement
- Local *"cyber militia"*
  - vigilantism ?
  - no warrant or protection at law

VICTIM B) RESPONSE - NCI

- International law
  - No adequate clarification of response
  - Even nation to nation



- Response illegal ?
  - Criminal code
  - Even to "clarify" attack
  - Automated counter-attack ?
    - Shut-down or partially disable attack system

16 May 2012 (c) W Caelli - IISEC Pty Ltd 41

VICTIM A) RESPONSE - BUSINESS

- Law enforcement
- Local "help" – defensive?
- Counter operations – illegal ?

16 May 2012 (c) W Caelli - IISEC Pty Ltd 42

RESPONSE TO THE CHALLENGE

TOLERATION

PASSIVITY

ATTACKER

LIMITED RESPONSE

ACTIVE RESPONSE

16 May 2012 (c) W Caelli - IISEC Pty Ltd 43

CYBER DEFENCE

- Who is defending ?
- What technology is used / managed ?
- Policy settings ?
- Legal situation ?

(Note: Even placement of passive monitors!)

16 May 2012 (c) W Caelli - IISEC Pty Ltd 44

CYBER DEFENCE

- military / intelligence entities
- law enforcement
- public / private / mixed enterprises
- NCI owner / operators
  - telecoms / common carrier
    (Telecommunications Act, Interception Act)
  - ISP (Note: NBN Australia)
- private sector – contractor
- SME – home user

CDC **Cyber** 70

CYBER DEFENCE

- Commonwealth Criminal Code Act 1995
- disrupt / destroy / interfere electronic systems
  - terrorism provisions
    - Section 100.1

Greg Farr (DoD Australia)

…he admitted that no one in the industry can have all of the skills that they need. "We're no longer in the business of employing all the IT specialists the business needs," he said. This makes partnering with industry necessary. (ZDNet.com.au 21 March 2012)

"Australian Cyber-warfare Centre"

Des Ball – 2008 (Strategic and Defence Studies Centre, ANU)

- *Its activities would be both defensive and offensive*
- *... research into possible vulnerabilities often suggests ways of exploiting these for offensive purposes.*
- *…..finding ways of penetrating the 'firewalls' protecting avionics systems and of using wireless application protocols (WAPs) to insert 'Trojan horses'.*
- *…..Scenarios would be continually researched and techniques practised to ensure the currency of the plans in contingent circumstances.*
- *A Cyber-warfare Centre would be responsible for identifying the preparations*
  - *… necessary for expeditious implementation of the plans, including the preparations for offensive operations.*

16 May 2012 (c) W Caelli - IISEC Pty Ltd 47

CYBER SECURITY AND THE "POSSE"

Research Questions:

- Could AusCERT and even CERTAustralia be "*posses*" at law?
  - Invocation (law enforcement officer ?)
  - Sworn officers? (deputies)
- Are private CERTs forms of "posse" or "vigilante" groups?
  - CERT as a commercial service ?
- What are legal implications for the entity and its members?

16 May 2012 (c) W Caelli - IISEC Pty Ltd 48

CHALLENGES:

- Does a form of *"posse"* have a place in the cyber-defence world ?
- Can traditional defence and law enforcement maintain the necessary staff and skills to cope with the cyber threat? (See US CAE program)
- Are *"cyber challenges"* really defence/law enforcement exercises?
- Are there new models?
- What are the legal, policy and political issues with concepts like a *"cyber militia"*?
- What can we learn from the concepts of *"militia"* ?
  - In Australia ?
  - In the USA ?

16 May 2012 (c) W Caelli - IISEC Pty Ltd 49

107TH CONGRESS
1ST SESSION

H. R. 3076

To authorize the President of the United States to issue letters of marque and reprisal with respect to certain acts of air piracy upon the United States on September 11, 2001, and other similar acts of war planned for the future.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 10, 2001

Mr. PAUL introduced the following bill; which was referred to the Committee on International Relations

LETTERS OF MARQUE

Thanks to Ms J Georgiades, QUT

CISSE The Colloquium for Information Systems Security Education

REMINDER

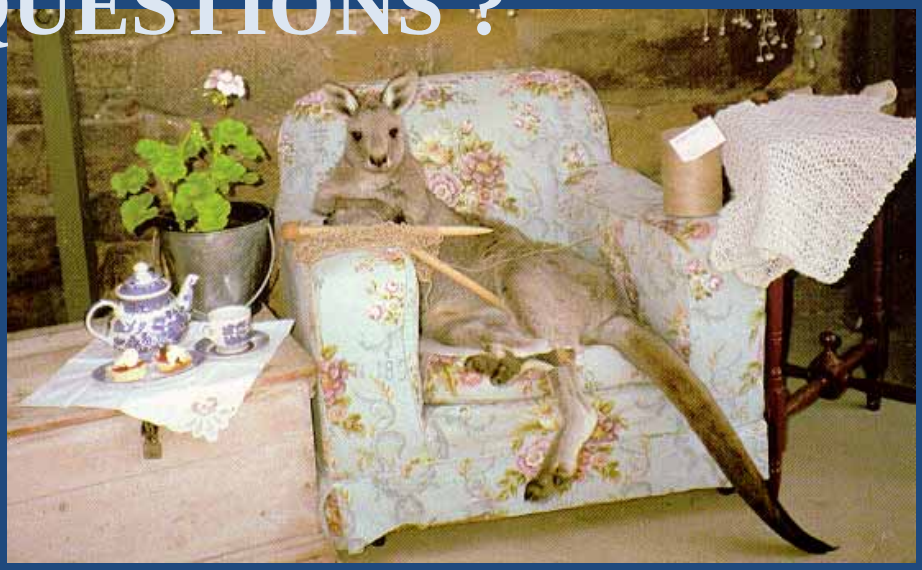
REGISTRATION IS OPEN

THE COLLOQUIUM 2012 LAKE BUENA VISTA, FL

Monday, June 11 - Wednesday, June 13, 2012

http://www.cisse.info

QUESTIONS ?



(Kangaroo courtesy Gay & David Epstein, Traveller's Rest, Cooma, NSW.)